SAND2017-1885R

Sandia National Laboratories

Datacenter Development: Risks, Mitigations, and Lessons Learned

D. J. Martinez and C. M. Keliiaa

Datacenter Development: Risks, Mitigations, and Lessons Learned
Risk: If the magnitude, vision, and path forward are not clearly defined prior to the start of a datacenter project, then the project may be subject to increased administrative risk due to insufficient planning.
Mitigation: Sufficient technical analysis, investment, and resource planning to ensure datacenter project milestones.
Lessons Learned: Analysis may indicate competitive advantage in datacenter design via secure and energy efficient designs, advancements in power cooling, virtualization, and computing; an organization should seek technical expertise through subject matter experts in respective fields and industry best practices.

Risk: If changes in leadership, vision, or priority interrupt multiyear commitment to datacenter development, then the project may be subject to increased administrative risk due to insufficient support.
Mitigation: Business continuity planning for long-term return-on-investment, including knowledge management and transfer of roles and responsibilities as necessary for successful leadership transition.
Lessons Learned: Stakeholder or leadership changes require transition processes for long-term return-on-investment.

Risk: If the market, job creation, and customer base objectives for datacenter service development are not clearly defined, then the project may be subject to increased administrative risk due to insufficient market placement.
Mitigation: Sufficient market analysis, investment, and resources allocated to assure successful datacenter market placement, job creation, and revenue supporting initial build and progressive datacenter infrastructure growth.
Lessons Learned: Market analysis provides insights for datacenter service industry investments and contingency investment for future operations; datacenters in themselves will not be a large employment factor after construction; return-on-investment and job creation may be augmented with digital service diversification (i.e. call centers).

Risk: If environmental, access, supply chain, and interjurisdictional dependencies are not clearly defined, then the project may be subject to increased operational risk due to insufficient identification of critical dependencies.
Mitigation: Sufficient analysis of water rights, power, accessible roads, network connectivity, flood plains, other hazards, and interjurisdictional dependencies to assure successful datacenter resilience of operations.
Lessons Learned: Resilient datacenter dependency analysis identifies efficiencies to enhance continuity of operations during periods of disruption due to variable environmental, access, facility, or human resource events.

Risk: If datacenter project requirements are not well defined and understood, then the project may be subject to increased operational risk due to insufficient requirements gathering, analysis, and tracking.
Mitigation: Sufficient requirements solicitation and third party objective review in the design phase.
Lessons Learned: Infrastructure, datacenter facility, and information and communications operational requirements need to be assessed to accommodate rapidly changing and emergent technologies.

Risk: If workforce knowledge, skills, and abilities do not meet datacenter requirements, then the project may be subject to increased operational risk of insufficient workforce preparedness.
Mitigation: Sufficient planning, investment, and workforce development to carry the datacenter project from planning, design, construction, initial build, to fully operational datacenter maintenance and operations.
Lessons Learned: Updated knowledge, skill, and abilities are necessary in infrastructure and facility areas of expertise; workforce development objectives will include cybersecurity and data governance.

Risk: If datacenter information security requirements are not clearly defined, then the project may be subject to increased technical risk due to an insufficient information security protection posture.
Mitigation: Sufficient requirements solicitation and third party objective review of requirements to include information categorization, valuation, and verification of protection mechanisms.
Lessons Learned: Rapidly changing information and communication technology increases complexity and risk; new technology deployments require built-in cybersecurity for an increased protection posture.

Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

2017-02-06

Sandia National Laboratories

Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

2017-02-06